Chapter 9

Secret Codes as Munitions and Money

Encryption Becomes Unbreakable

9.1 Senator Gregg Reconsiders

September 13, 2001: Fires were still smoldering in the wreckage of the World Trade Center when Judd Gregg of New Hampshire rose to tell the Senate what had to happen. He recalled the warnings issued by the FBI years before the country had been attacked: that the FBI's most serious problem was "the encryption capability of the people who have an intention to hurt America." "It used to be," the senator went on, "that we had the capability to break most codes because of our sophistication."[1] No more. "The technology has outstripped the code breakers,"[2] he warned. Even civil libertarian cryptographer Phil Zimmermann agreed that the terrorists were probably encoding their messages. Zimmermann's software had been posted on the Internet in 1991 for use by human rights workers around the world, but he had to acknowledge that the bad guys also "would want to hide their activities using encryption."[3]

Encryption is the art of encoding messages so they can't be understood by eavesdroppers or adversaries into whose hands the messages might fall. De-scrambling an encrypted message requires knowing the sequence of symbols—the "key"—that was used to encrypt it. An encrypted message may be visible to all the world, but without the key, it may as well be hidden in a locked box.

What was needed, Senator Gregg asserted, was "the cooperation of the community that is building the software, producing the software, and building the equipment that creates the encoding technology." Cooperation, that is, enforced by legislation. Whoever made encryption software, Senator Gregg proposed, would have to enable the government to bypass the locks and retrieve the decrypted messages. What about encryption programs written abroad, which could be shared around the world in the blink of an eye, as Zimmermann's had been? The US should use "the market of the United States as leverage" in getting foreign manufacturers to follow requirements for "back doors" that could be used by the US government.

By September 27 Gregg's legislation was beginning to take shape. The keys used to encrypt messages would be held in escrow by the government under tight security. There would be a "quasi-judicial entity," appointed by the Supreme Court, that would decide when law enforcement had made its case for release of the keys. Civil libertarians squawked, and doubts were raised as to whether the key escrow idea could actually work. No matter, opined the Senator in late September. "Nothing's ever perfect. If you don't try, you're never going to accomplish it."[4]

And then abruptly, Senator Gregg dropped his legislative plan. "We are not working on an encryption bill," said the Senator's spokesman on October 17.[5]

On October 24 Congress passed the USA PATRIOT Act, giving the FBI sweeping new powers to combat terrorism. But the PATRIOT Act does not even mention encryption. No serious attempt has been made to legislate control over cryptographic software since Gregg's proposal. Why not?

9.2 Why Not Regulate Encryption?

Throughout the decade of the 1990s, the FBI had made control of encryption its top legislative priority. Senator Gregg's proposal was a milder form of a bill, drafted by the FBI and reported out favorably by the House Select Committee on Intelligence in 1997, that would have mandated a five-year prison sentence for selling encryption products unless they enabled immediate decryption by authorized officials.[6]

How could regulatory measures deemed critical for fighting terrorism by US law enforcement in 1997 drop completely off the legislative agenda four years later—in the aftermath of the worst terrorist attack ever suffered by the United States of America?

No technological breakthrough in cryptography in the fall of 2001 had legislative significance. There were no diplomatic breakthroughs either. Nothing else transpired to make the use of encryption by terrorists and criminals unimportant. It was just that something else about encryption had become *more* important. And that was to ensure that encryption tools could be in the hands of banks and their customers, airlines and their customers, Ebay and Amazon and L. L. Bean and their customers. That is, in the hands of anyone using the Internet for commerce.

For a decade, government officials had been debating the tension between secure conduct of electronic commerce and secret communication among outlaws. Senator Gregg was but the last of the voices calling for restrictions on encryption. The National Research Council had issued a report of nearly 700 pages in 1996 weighing the alternatives. The report concluded that on balance, efforts to control encryption would be ineffective, and that their costs would exceed any imaginable reward.[7] The intelligence and defense establishment remained unpersuaded. FBI Director Louis Freeh testified before Congress in 1997 that uncontrolled public access to encryption "ultimately will devastate our ability to fight crime and prevent terrorism."[8]

Yet only four years later, even in the face of the September 11th attack, electronic commerce demanded encryption software for every business in the country and every home computer from which a commercial transaction might take place. At the moment when Freeh was cautioning

Congress about encryption software, elected officials might never have bought anything on line and their families might never have used computers. By 2001, computers had become consumer appliances, Internet connections were common in American homes—and average citizens were well aware of electronic fraud. Consumers did not want their credit card numbers and social security numbers exposed to everyone on the Internet.

Why is encryption so important to Internet communications that Congress was willing risk terrorists using encryption, so that American businesses and consumers could use it too? After all, information security is not a new idea. People communicating by postal mail have reasonable assurances of privacy without any use of encryption.

The Internet is different from the postal system, despite the metaphor of electronic "mail." Data packets zipping across the Net are not like envelopes with an address on the outside and contents sealed inside. Packets are more like postcards, with everything exposed for anyone to see. Every data packet passing through the Internet gets handled at every router: stored, examined, checked, analyzed, and sent on its way. The routers are not under any form of central control or security certification. Even if the routers could be controlled and all the fibers and wires subject to wiretap regulations, wireless networks allow bits to be grabbed out of the air without detection. Indeed, by 2001, a lot of bits were traveling though the air, and snoopers could easily look at them.

The way to make Internet communications secure—to make sure that no one but the intended recipient knows what is in a message—is for the sender to encrypt the information so that only the recipient can decrypt it. If the contents of data packets are encrypted, then routers, sniffers, and eavesdroppers along the route from sender to receiver can examine the packets all they want. All they will find is an undecipherable scramble of bits.

In 2001, electronic commerce accounted for less than 1% of retail sales in the US. That percentage has grown to 3% today, around $130 billion. A great deal of the money that fuels the American economy now moves from consumers to businesses, and between businesses, only as bits. Altering those bits would be tantamount to stealing money.[9]

As the world awakened to Internet commerce, encryption could no longer be thought of as it had been from ancient times until the turn of the third millennium: as armor used by generals and diplomats to protect information critical to national security. Suddenly, encryption was more like the armored cars used to transport cash on city streets, except that *everyone* needed these armored cars. Encryption was no longer a munition; it was more like money.

The commoditization of a critical military tool was more than a technology shift. It sparked reconsideration of fundamental notions of privacy and of the tension between security and freedom in a democratic society.

"The question," posed MIT's Ron Rivest, one of the world's leading cryptographers, during one of the many debates over encryption policy, "is whether people should be able to conduct private conversations, immune from government surveillance, even when that surveillance is fully authorized by a Court order."[10] By 2001 commercial realities had overtaken such debates. The same technology that protects your credit card numbers when you place an order over the web also enables you to conspire to overthrow the government without the government knowing what you are saying.